

PAT-NO: JP02000132610A

DOCUMENT-IDENTIFIER: JP 2000132610 A

TITLE: USER IDENTIFYING METHOD AND IC CARD

PUBN-DATE: May 12, 2000

INVENTOR-INFORMATION:

NAME	COUNTRY
NAKASHIGE, AKIRA	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI SOFTWARE ENG CO LTD	N/A

APPL-NO: JP11331796

APPL-DATE: February 2, 1999

INT-CL (IPC): G06F017/60, G07F007/12

ABSTRACT:

PROBLEM TO BE SOLVED: To allow an IC card side to receive and certify password information provided for an IC card user without increasing the burden such as the user's memory and safely against tapping action.

SOLUTION: Both of a password information receiving program and a password information certifying program are held in the IC card as a pair. At the time of certifying the user of the IC card, the password information receiving program is loaded from the IC card 12 to a terminal device 13, which transmits/receives information between the IC card 12 and its user, to execute. Thus, a display picture for inputting password information is displayed on a display attached to the device 13 and user password information inputted through this display picture for inputting password information is transferred to the password information certifying program operating in the IC card 12 from the password information receiving program to certify the propriety of user password information.

COPYRIGHT: (C)2000,JPO

DERWENT-ACC-NO: 2000-392046

DERWENT-WEEK: 200034

COPYRIGHT 1999 DERWENT INFORMATION LTD

TITLE: User authentication procedure for IC card, involves
authenticating correctness of code and allows user to
change incorrect native information

PATENT-ASSIGNEE: HITACHI SOFTWARE ENG CO LTD[HISF]

PRIORITY-DATA: 1998JP-0079349 (March 26, 1998)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
JP 2000132610 A	May 12, 2000	N/A	014	G06F 017/60

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
JP2000132610A	Div ex	1999JP-0024860	February 2, 1999
JP2000132610A	N/A	1999JP-0331796	February 2, 1999

INT-CL (IPC): G06F017/60, G07F007/12

RELATED-ACC-NO: 2000-211387

ABSTRACTED-PUB-NO: JP2000132610A

BASIC-ABSTRACT:

NOVELTY - An IC card (12) stores native language information of an user and a process program. The code from IC card is read and the native language information is processed and displayed in screen display device (23). An user chooses any incorrect information from displayed native information and the correctness of user code information is authenticated.

USE - For transaction of money using IC card.

ADVANTAGE - The code informations cannot be misused during domestic utilization or international commercial transaction and hence burden to user is reduced.

DESCRIPTION OF DRAWING(S) - The figure shows the exterior block diagram of

terminal apparatus for IC card.

IC card 12

Screen display device 23

CHOSEN-DRAWING: Dwg.2/15

TITLE-TERMS: USER AUTHENTICITY PROCEDURE IC CARD AUTHENTICITY
CORRECT CODE

ALLOW USER CHANGE INCORRECT NATIVE INFORMATION

DERWENT-CLASS: T01 T04 T05

EPI-CODES: T01-H01B3A; T01-J05A1; T01-J12C; T04-K01; T05-H02C5C;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N2000-293942

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-132610

(P2000-132610A)

(43)公開日 平成12年5月12日(2000.5.12)

(51)Int.Cl.⁷

識別記号

F I

テマコード*(参考)

G 0 6 F 17/60

G 0 6 F 15/21

3 4 0 B

G 0 7 F 7/12

G 0 7 F 7/08

B

審査請求 有 請求項の数 5 O L (全 14 頁)

(21)出願番号 特願平11-331796
(62)分割の表示 特願平11-24860の分割
(22)出願日 平成11年2月2日(1999.2.2)

(31)優先権主張番号 特願平10-79349
(32)優先日 平成10年3月26日(1998.3.26)
(33)優先権主張国 日本(J P)

(71)出願人 000233055
日立ソフトウェアエンジニアリング株式会
社
神奈川県横浜市中区尾上町6丁目81番地
(72)発明者 中重 亮
神奈川県横浜市中区尾上町6丁目81番地
日立ソフトウェアエンジニアリング株式会
社内
(74)代理人 100083552
弁理士 秋田 収喜

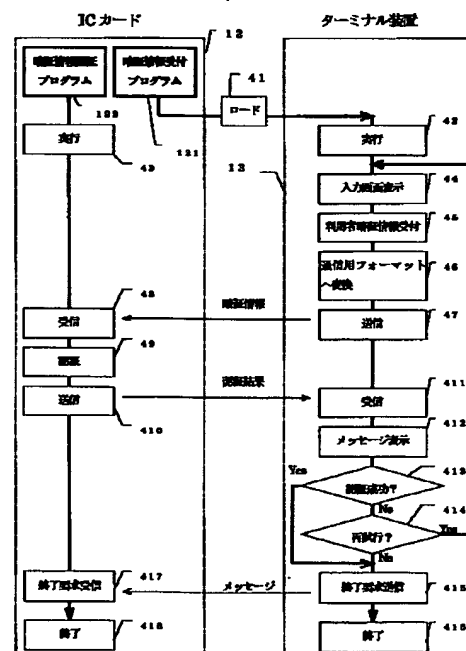
(54)【発明の名称】 利用者認証方法およびICカード

(57)【要約】

【課題】 ICカード利用者のみが持つ暗証情報を、利用者の記憶等の負担を増やすことなく、しかも盗聴行為に対して安全にICカード側で受け取り、認証する。

【解決手段】 ICカード内に暗証情報受付プログラムと暗証情報認証プログラムの両者をペアで保持し、ICカード利用者を認証する際に、ICカードとの間で情報を送受するターミナル装置に対し、前記暗証情報受付プログラムをICカードからロードして実行させることによって、ターミナル装置に付随する表示装置上に暗証情報入力用表示画面を表示させ、この暗証情報入力用表示画面を通して入力された利用者暗証情報を前記暗証情報受付プログラムからICカード内で動作する暗証情報認証プログラムに転送し、利用者暗証情報の正当性を認証する。

図 4



【特許請求の範囲】

【請求項1】 マイクロプロセッサを搭載したICカードを用いて商取引引き用の利用者を認証する利用者認証方法であって、

利用者の母国語情報とそれを加工する加工プログラムとをICカード内に保持し、ICカード利用者を認証する際に、利用者個人の暗証情報を入力する手続きに先立ち、前記加工プログラムにより前記母国語情報を加工し、その加工後の母国語情報をICカードとの間で情報を送受するターミナル装置の表示装置上に表示させ、その表示された母国語情報の中の正しいものまたは誤っているものを利用者を選択させ、その結果に基づいて利用者の正当性を認証することを特徴とする利用者認証方法。

【請求項2】 予め特定に母国語文字グループをICカード内に登録しておき、利用者固有の認証を行うことを特徴とする請求項1記載の利用者認証方法。

【請求項3】 商取引引き用の利用者認証に使用するマイクロプロセッサ搭載のICカードであって、ICカードを認証する際に、利用者の母国語情報を加工し、その加工後の母国語情報をICカードとの間で情報を送受するターミナル装置の表示装置上に表示させ、その表示された母国語情報の中の正しいものまたは誤っているものを利用者を選択させる加工プログラムと、その選択結果に基づいて利用者の正当性を認証する認証プログラムとを保持していることを特徴とするICカード。

【請求項4】 マイクロプロセッサを搭載したICカードを用いて商取引引き用の利用者を認証する利用者認証方法であって、

利用者のよく知っている地域情報とそれを加工する加工プログラムとをICカード内に保持し、ICカード利用者を認証する際に、利用者個人の暗証情報を入力する手続きに先立ち、前記加工プログラムにより前記地域情報を加工し、その加工後の地域情報をICカードとの間で情報を送受するターミナル装置の表示装置上に表示させ、その表示された地域情報の中の正しいものまたは誤っているものを利用者を選択させ、その結果に基づいて利用者の正当性を認証することを特徴とする利用者認証方法。

【請求項5】 商取引引き用の利用者認証に使用するマイクロプロセッサ搭載のICカードであって、ICカードを認証する際に、利用者のよく知っている地域情報を加工し、その加工後の地域情報をICカードとの間で情報を送受するターミナル装置の表示装置上に表示させ、その表示された地域情報の中の正しいものまたは誤っているものを利用者を選択させる加工プログラムと、その選択結果に基づいて利用者の正当性を認証する認証プログラムとを保持していることを特徴とするICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカードを利用して電子マネー等を扱う場合に好適な利用者認証方法に関するものである。

【0002】

【従来の技術】ICカードを利用して電子マネーを扱う商取引システムでは、セキュリティの確保が重要な課題である。特に、ICカードを汎用の電子財布やクレジットカードとして利用する際には、正当なカード利用者の認証が様々な電子マネーの支払・受取の状況で行われることになるが、これらの状況において、この認証方法を十分に安全なものにしておく必要がある。

【0003】様々な状況で頻繁にICカードを利用する際には、ICカードからデータの出し入れを始めるための初期処理の部分で、悪意を持った人間が不正な手段によって利用者認証をすり抜けてしまうことが可能であれば、電子マネーのデータ自体を頑強に保護するどのような技術を駆使しても無駄になってしまう。

【0004】現在、一般的に利用者が限定されて広く使われているカードとしては、クレジット会社の発行するクレジットカードや銀行の発行するキャッシュカードなどがあるが、それぞれの利用者認証に関しては、前者は筆記による署名、後者はキャッシュディスペンサ装置での4桁程度の暗証番号の入力が一般的である。

【0005】しかしながら、ICカードを用いて電子マネーを保持し、それを物品の購買等に利用する状況では、ICカードの内部に貨幣価値をもつデータを持っているため、盗難時の保証などの観点から、より厳しい利用者認証技術が必要である。

【0006】特に、ICカードから電子マネーのデータを出し入れするための端末は、銀行のキャッシュディスペンサ装置のように限定された安全な状況・装置になるとは限らず、レストラン、スーパーマーケット、駅の売店、タクシー、アミューズメントセンターなど、使用状況も装置も様々なものになる可能性がある。

【0007】さらに、各小売店などが用意するICカード用のターミナル装置も、ICカード発行者が指定した特定の装置になるとは限らず、むしろ様々な商取引サービスに対応したいろいろなICカードを受け付ける共用の装置が設置される可能性があり、これも必ずしも安全とは限らない。例えば、ターミナル装置の内部に利用者の暗証番号を盗むための仕組みが組み込まれる危険性もある。

【0008】以上のように、ICカード内に電子マネーを保持して商取引を行うことが日常的に広まれば、従来のクレジットカードやキャッシュカードとは異なる、安全性の確保されていない条件下で正当なカード利用者を認証しなければならない状況が増えてくる。

【0009】従来の利用者認証技術としては、(1)

50 暗証番号、(2) 署名、(3) 指紋、(4) 声紋、

(5) 網膜パターン、といった利用者固有の情報に基づいたものが知られており、研究段階のものから実用段階のものまで様々なレベルにある。

【0010】このうち(1)の暗証番号を使用するものは、既に銀行のキャッシュカードなどで実用化されている方法であるが、広く一般に使用が可能である必要性から、4桁程度の数字が普通設定されているデータの量である。この方法で更に安全性を高めるには、暗証データの桁数を増やせばよいが、これには利用者の記憶に負担を強いることになる。

【0011】次に、(2)の署名を使用するものは、デジタル化されたものではないが、クレジットカードなどで実際に利用されており、認証する側の人間が目視で判断している。これをデジタル化した場合、カード用の全てのターミナル装置に署名のための特殊な装置を付属する必要があり、コスト面で普及への障害となる。また、判定のアルゴリズムもデータの類似性を判断する必要があり、模倣による差異を区別するための処理が問題である。

【0012】次に、(3)の指紋、(4)の声紋、(5)の網膜パターンなどのバイオメトリクスを使用するものは、利用者の身体的特徴をデータとして扱うものであるが、これらも署名を使用する方法と同様の問題がある。また、精度を上げるためにはそれぞれのデータ毎に特殊な装置を付加する必要も出てくる。例えば、声紋を使用する方法では音声情報から利用者個人に特有な特徴量を算出するためのプロセッサやソフトウェアなどが必要であり、また網膜パターンを使用する方法では網膜を読み取る装置がまず最初に必要になる。したがって、これらの情報を一般の商取引の現場でICカード向けの利用者認証に応用するには困難な点が多い。

【0013】一方、最近では、電子マネーを扱う商取引システムでICカードを利用する場合、これまでの磁気カードのようにデータを保存するためだけの受動的媒体としてではなく、ICカード内にOS(オペレーティングシステム)を用意し、商取引のためのアプリケーションプログラムをICカードOSの上で動作させ、商取引に関連するサービスを行う能動的なカードとして利用するものが、登場している。

【0014】この能動的なICカードに対する利用者認証の技術で、利用者の利用状況までを考慮したものとしては、例えば、特開昭62-37198号に開示された技術がある。これは、ICカードケースから予め暗証番号を入力しておき、電車の改札口などで短時間内に電子マネーのやり取りを可能にするものであるが、安全に利用するには予め利用金額が決まっているか小額である状況に限定されると考えられるので、様々な商取引の状況に対応した認証方法ではない。

【0015】また、盗難などで利用権限のないものがICカードを入手し、これを利用しようと試みた際の防御

技術としては、特開昭61-151793号に開示された技術がある。これは、認証用データとの照合の失敗回数をカード側でカウントして、規定回数以上になるとカード自身で自分の持つデータの流出を防止するものである。従って、カードの盗難後に認証情報自体の類推処理を妨げることが可能であるが、カード利用時の盗聴を防止するものではない。

【0016】一方、今後、クレジットカード等に代り、このようなICカードが国際的な状況において電子商取引に利用されて行く予想されるが、海外での利用では、特にICカードとデータをやり取りするターミナル装置の信用に問題がある。世界各地のそれぞれの事情・状況において、カード利用に伴うリスクは程度が異なっており、例えばターミナル装置に改造が加えられ、利用者の暗証情報が盗聴できるようになっているなど、国内とは異なるリスクの可能性がある。

【0017】

【発明が解決しようとする課題】本発明は、このような事情を解決すべくなされたものであり、その目的は、国内利用においても、あるいは海外利用などの国際的取引きであっても、ICカード利用者のみが持つ暗証情報を、利用者の負担を増やすことなく、しかも盗聴行為に対して安全にICカード側で受け取り、認証するための利用者認証方法を提供することにある。

【0018】

【課題を解決するための手段】上記の目的を達成するために、本発明は、ICカード内に、海外利用時のカード利用者認証の機能を持たせる。具体的には、母国語情報(母国が日本ならば、日本語情報)と、それを加工するプログラムをカード内に保持させ、海外でのカード利用者認証の際に、個人の暗証情報を入力する手続きに先立って、母国語情報に基づく認証手続きを行う。

【0019】例えば、日本語情報としては、日常的に利用しているひらがな・カタカナ・漢字などを用いる。利用者認証の際には、ICカード内の加工プログラムで幾つかの文字(例えば10文字程度)を選択し、その一部を加工して日本語にはない文字を幾つか生成し、ターミナル装置上で表示する。加工の仕方としては、漢字の部首をとり替えたり、濁点・半濁点などを付加するなどして、正しくない文字を生成する。カード利用者は、加工して作られた正しくない文字または正しい文字を、ターミナル装置上で選択することで、正当な利用者であることをICカード内の認証プログラムに対して伝える。

【0020】また、カード利用者固有の設定として、予め特定の文字グループ(例えば、にんべんの付く漢字など)を指定しておき、利用者認証時に、これらも正しくない文字または正しい文字としてターミナル装置上で選択させる。

【0021】このような手段を講じることにより、母国語として日本語を日常利用しているカード利用者にとっ

ては、記憶しておくべき情報はほとんど増えず、また加工された文字はビジュアル的に誤りを判定できるため、負担が極めて軽いものである。一方、外国人にとっては日本語を習得し、またその誤りを速断できる能力を獲得するのは非常に困難であるため、カード盗難の際にも不正使用されるリスクを減らす効果がある。

【0022】また、本発明は、ＩＣカード内に、利用者固有の情報に基づくカード利用者認証の機能を持たせる。具体的には、利用者が特に詳しく知っている地域情報とそれを加工するプログラムをカード内に保持させ、利用者の認証手続きを行う。

【0023】例えば、地域情報としては、出身地、職場周辺、出身学校周辺などを選択し、予め選んだ地域内のデータをＩＣカード内に貯えておく。

【0024】出身地や職場などの地域の情報は、多くの人に共有されており、地域情報に詳しい人は当該ＩＣカード利用者だけではないが、地域を複数個（例えば、出身地、職場周辺、親戚が住む町、などの３地域）選択しておくことにより、選択したすべての地域に詳しい人物がほとんど当該ＩＣカード利用者だけになるようにしておく。

【0025】地域内のデータとしては、地名、町名、自然物（山や川の名前）、観光スポット名などを対象とし、その地域に居住したり、通勤、通学などの経験で自然と身につく情報を選ぶ。これらの情報は、例えばカーナビゲーションシステムなどのデジタル化された地図情報システムから、一部分を選択することにより容易に得ることができる。

【0026】利用者認証の際には、ＩＣカード内の加工プログラムで上記地域内のデータの幾つかを選択し、さらにその中の一部または全部を加工して、ターミナル装置上で表示する。加工の仕方としては、名称中の文字の一部取り替えたり、読み方、表記法を変えたりするなどして、正しくない名称を生成する。ＩＣカード利用者は加工して作られた地域内の正しくない名称または正しい名称をターミナル装置上で選択することで、正当な利用者であることをＩＣカード内の認証プログラムに対して伝える。

【0027】このような手段を講じることにより、自らの経験から習得した地域情報を当たり前のものとして記憶しているカード利用者にとっては、新たに記憶すべき情報はほとんど増えず、また加工された地域内の名称は即座に誤りを判定できるため、負担が極めて軽いものである。一方、当該ＩＣカード利用者以外の人にとっては、選択された複数の地域のすべてについてその情報を習得し、またその誤りを速断できる能力を獲得するのは非常に困難であるため、カード盗難の際にも不正使用されるリスクを減らす効果がある。

【0028】

【発明の実施の形態】以下、図を用いて本発明の一実施

形態について説明する。図１は、本発明のＩＣカード向け利用者認証方法を実施する場合のサービス提供者１１、ＩＣカード１２、ＩＣカード向けターミナル装置１３の関係を示した図である。図１においては、例えば、サービス提供者１１である「銀行Ａ」が、当該銀行に口座を持つ「ＩＣカード利用者Ｂ」に、その利用者Ｂ所有のＩＣカード１２に対して電子マネーを出し入れするサービスを提供する場合、あらかじめ、ＩＣカード１２へ「暗証情報受付プログラム」と「暗証情報判定プログラム」をベアで配布しておく。

【0029】このプログラムの配布は、「銀行Ａ」の支店内・キャッシュディスペンサ装置の設置場所や利用者の自宅内のパーソナルコンピュータを利用する状況など、安全性の確保された環境で実施する。

【0030】「銀行Ａ」の提供するサービスに対応したベアのプログラムを配布されたＩＣカード１２を持つ「ＩＣカード利用者Ｂ」は、ＩＣカード１２内に保持している電子マネーを使って、ＩＣカード向けターミナル装置１３の設置してある「小売店Ｃ」で物品などを購入することが出来る。

【0031】図２は、ＩＣカード向けターミナル装置１３の一例を示す外觀図である。ここでは、電話機をベースに機能拡張して、ＩＣカード用のスロット２１が用意したものを示している。このスロット２１にＩＣカード１２を挿入することで、ＩＣカード１２とターミナル装置１３の間で、電子マネーやその他のデータがやり取り出来るようになっている。

【0032】本実施形態では、暗証情報の入力をテンキー装置２２によって入力するのではなく、画面表示装置２３上を使って入力するようにしている。図２では、画面表示装置２３がタッチスクリーンになっており、ＩＣカード利用者Ｂはタッチスクリーンに表示されたオブジェクトに触れる、あるいは押圧することでオブジェクトを選択する。

【0033】なお、表示されたオブジェクトを選択する手段としては、マウス、トラックボール、タッチパッド等を使ったものが考えられるが、本発明は、この選択手段の種類を限定するものではない。

【0034】図３は、ターミナル装置１３にＩＣカード１２を挿入してから、電子マネーを扱う取引までの手順の概要を示したフローチャートである。まず、電子マネーを支払う側のＩＣカード１２は、まずターミナル装置１３が正しい規格にあったものかどうかを判定し（ステップ３１）、正しい規格であることが認証できた場合には、次にＩＣカード１２の利用者が正当な利用者であるかを判定する（ステップ３２）。これらのチェックに合格したのち、ＩＣカード１２は電子マネーをターミナル装置１３へ提供して取引処理終了（ステップ３３）となり、スロット２１から排出され、利用者に返却される。

【0035】ここで、ステップ３１、３２におけるチェ

ックに合格しなかった場合は、ICカード12側が判断して、電子マネーを使った商取引を許可しない。本発明は、この手順の中で、ステップ32のICカード利用者の認証段階に関するものである。

【0036】図4は、このICカード利用者の認証の手順を、ICカード12内に組み込んだ「暗証情報受付プログラム」121と「暗証情報認証プログラム」122の動作から詳細に示したものである。

【0037】まず、ICカード12をターミナル装置13のスロット21へ挿入すると、「暗証情報受付プログラム」121がICカード12からターミナル装置13へとロードされ（ステップ41）、ターミナル装置13内での実行が開始される（ステップ42）。同時に「暗証情報認証プログラム」122がICカード上で動作し始め（ステップ43）、ターミナル装置13内にロードされた「暗証情報受付プログラム」121と通信によりデータを交換する。

【0038】これらのプログラムのロード・実行・通信は、例えばJava仮想マシンとJavaアプレットの配信機構をICカード12とターミナル装置13に実装しておけば容易に実現できる。ただし、本発明は特定のプログラミング言語やプログラムのロード方式、実行方式に限定したものではない。

【0039】ターミナル装置13内で動作を始めた「暗証情報受付プログラム」121は、ターミナル装置13の画面表示装置23に認証情報入力用の画面を表示する（ステップ44）。本実施形態では、画面表示装置23をタッチスクリーンとしているので、ICカード利用者はこの画面に触れる、あるいは押圧することによって、暗証情報を入力する（ステップ45）。

【0040】図5は、「暗証情報受付プログラム」121によって表示された認証情報入力用の画面の一例を示す図である。「暗証情報受付プログラム」121は、様々な取引サービス毎に配布されたものであるため、生成される画面も取引種別やサービス毎に異なるように特定の管理者あるいはメーカーにおいて任意に生成することができる。このため、この例ではサービス名をタイトル位置に表示するエリア51を設けている。また、暗証情報をこれまで何個入力したかを確認するため「*」印などの数で表示する為のエリア52、暗証情報を入力し終ったことを確定するためのOKボタン53、入力途中で間違ってしまったときにやり直すためのキャンセルボタン54、ICカード12上で動作している「暗証情報認証プログラム」122からのメッセージを表示するためのエリア55も用意してある。

【0041】暗証情報自体の入力に関して、この例では、様々な「図形」（△、○、☆など）のオブジェクトが生成されて表示されている。これらの「図形」の位置は毎回ランダムに生成され、その都度、表示位置が変わり、選択操作位置を他人に知られたとしても、選択した

オブジェクトそのものが知られなければ、暗証情報が分からないように工夫してある。表示されるオブジェクトは「図形」に限らず、「数字」、「アルファベット」、「日本語（漢字・平仮名・カタカナ）」を代わりに利用することも可能である。さらにオブジェクトに色や大きさのランクを設けて、バリエーションを付けることが可能である。

【0042】さらに、これらのオブジェクトを静的に表示するだけではなく、それぞれを動かして表示することでバリエーションを付けることが可能である。これらのいかなる場合でも、「暗証情報受付プログラム」121はどの位置にどのオブジェクトを表示しているかを管理しているので、ICカード利用者が選択したオブジェクトを特定することが可能である。

【0043】一方、ICカード利用者が覚えるべき暗証情報自体は、これらのオブジェクトの特定の属性に着目したもので、4個程度の並びとして予め登録しておく。

【0044】例えば、

- (1) △→□→○→☆
- (2) 緑→赤→黄→紫
- (3) 大→小→中→極大

などを暗証情報とすることができる。

【0045】このような暗証情報を設定しおけば、ICカード利用者は通常銀行のキャッシュカードの暗証番号を覚えるのと同程度の負担で、複雑な暗証情報を利用できる。

【0046】一方で、バリエーションの豊かな認証情報入力用の画面を利用することにより、暗証情報を入力する際にまわりにいる人間に情報を盗まれる可能性や、ターミナル装置13に隠された装置で盗聴される可能性を非常に少なくできる。

【0047】図5のような認証情報入力用の画面を通じてICカード利用者から入力された認証情報は、通信用のデータフォーマットに変換され（図4のステップ46）、ICカード12上で動作している「暗証情報認証プログラム」122へ送信される（ステップ47）。

【0048】図6は、2つのプログラム121、122の間で受け渡される暗証情報のデータフォーマットの例である。

【0049】これは、入力されたオブジェクトの並びを順番に繋げただけのものだが、どの属性値の並びが実際に有効な暗証情報であるか、ターミナル装置13側には分からないようになっている。

【0050】さらに安全な受渡しをするには、2つのプログラム121、122間で秘密鍵を予め用意しておき、この通信用のデータを「暗証情報受付プログラム」121で暗号化して送信し、「暗証情報認証プログラム」122で受信の後、復号化する構成にすることも可能である。

【0051】なお、本実施形態では「暗証情報受付プロ

グラム」121と「暗証情報認証プログラム」122の間で暗証情報をまとめて受け渡しているが、本発明は、ICカード利用者から入力される暗証情報の受渡しをこのような2つのプログラムの同期したものに限したものではなく、2つのプログラムが非同期に動作することがあってもよい。

【0052】暗証情報を受信した「暗証情報認証プログラム」122は、データフォーマットに従ってその内容が正しいものであるかどうかを認証し(図4のステップ48、49)、その結果を伝えるメッセージを「暗証情報受付プログラム」121に対して送信する(ステップ410)。ここで、暗証情報の認証を行うプログラムコード自体はICカード12の中にあり、そこで動作するため、ターミナル装置13側でコピーを取られて逆アセンブルなど、そのアルゴリズムを解析される恐れがない。

【0053】判定結果のメッセージを受信した「暗証情報受付プログラム」121は、そのメッセージ内容を、認証情報入力用の画面内に用意しておいたメッセージ用のエリア55に表示する(図4のステップ411、412)。

【0054】この後、メッセージ内容を判定し(ステップ413)、入力された暗証情報が正しく、認証が成功した場合は、2つのプログラムとも終了する。また、認証が失敗した場合は、さらに「ある決まった回数まで」などの条件を判定し(ステップ414)、再度ICカード利用者から暗証情報の入力を受けつける。2つのプログラム121、122が終了する際には、同期を取るために「暗証情報受付プログラム」121から「暗証情報認証プログラム」122に対して終了要求のメッセージを送信し(ステップ415)、終了する(ステップ416)。一方の「暗証情報認証プログラム」122は、この終了要求メッセージを受信した後(ステップ417)、終了する(ステップ418)。

【0055】以上の説明から明かなように、本実施形態によれば、ICカード12を利用した商取引サービスにおいて、以下の特徴を持つ、ICカードの利用者認証方法を実現することが可能である。

(1) ICカード12を利用する商取引の様々な状況において暗証情報を盗むことが困難である。特に、ICカード用ターミナル装置13に細工がしてあっても安全である。

(2) ターミナル装置13に付加すべき暗証情報読み取り用装置として、特定の暗証情報の種類に特化した特殊装置を必要としない。

(3) 暗証情報の増加や複雑化に伴う利用者への負担を増やさない。

(4) サービス毎に認証方法を自由に取り替えられる。

【0056】これらの特徴は、ICカード12を利用す

る状況が、レストラン、スーパーマーケット、駅の売店、タクシー、アミューズメントセンターなど、一律にセキュリティの水準を確保することが困難な、様々なものへと広まった際に、特に有効である。

【0057】次に、本発明の第2の実施形態について説明する。この第2の実施形態は、特にICカードの国際的な利用状況を考慮し、海外の小売店Cで電子マネーの取引を行う場合を想定したものであり、例えば、サービス提供者11の「銀行A」が講座を持つ「ICカード利用者B」に、そのICカード12に対して電子マネーを出し入れするサービスを提供する場合、あらかじめ、ICカードへ「日本語情報」と「日本語情報加工プログラム」を配布しておくものである。この場合、日本人向けでない場合は、ICカード所有者の「母国語情報」と「母国語情報加工プログラム」とを配布するものである。以下、ICカード利用者は日本人であるものとして説明する。

【0058】この「日本語情報」および「日本語情報加工プログラム」の配布は、「銀行A」の支店内・キャッシュディスペンサ装置の設置場所や利用者の自宅内のパーソナルコンピュータを利用する状況など、安全性の確保された環境で実施する。

【0059】「日本語情報」と「日本語情報加工プログラム」を配布されたICカード12をもつ「ICカード利用者B」は、ICカード12内に保持している電子マネーを使って、ICカード向けターミナル装置13の設置してある「小売店C」で物品などを購入することが出来る。本実施形態では、特にICカードの国際的な利用状況を対象とし、この「小売店C」を海外のものと想定している。「小売店C」に設置されるターミナル装置13は、図2と同様の構成になっており、スロット21にICカード12を挿入することで、ICカード12とターミナル装置13の間で、電子マネーその他のデータがやり取りできるようになっている。

【0060】本実施形態では、利用者認証用の確認データや個人の暗証情報の入力を、テンキー装置22によって入力する。利用者認証のための日本情報は、画面表示装置23上で表示する。

【0061】なお、第1の実施形態の場合と同様に、画面表示装置23をタッチスクリーンとして、ICカード利用者が触れる、あるいは押圧することにより、表示された文字等を選択してもよい。他にも選択する手段は、マウス、トラックボール、タッチパッド等を使ったものが考えられるが、本発明は、この選択手段の種類を限定するものではない。

【0062】図7は、ICカード内12に保存しておく「日本語情報」71の例である。文字を単位として扱い、日常的に利用しているものが選択されて格納されている。文字については、文字のイメージ情報の他に、部首や画数など、通常の国語辞典・漢和辞典等に掲載され

10

20

30

40

50

ている情報の一部を使って、幾つかのグループを用意し、各々のエントリがどのグループに属しているかという情報も持っている。

【0063】図7で示す「日本語情報」に対するグループの例としては、

- (1) にんべんのつく漢字
- (2) 草冠のつく漢字
- (3) 濁点のつくカタカナ
- (4) 4画以下の漢字

などが考えられる。

【0064】図8は、「日本語情報加工プログラム」により正しい「日本語情報」から明らかに誤りと判定できる文字イメージを生成した例である。ここでは、濁点や半濁点などが付かない筈のひらがな、カタカナに付加したり、漢字の一部を加工している。日本語を母国語とするICカード利用者が、即座に正誤が判定できるような誤った文字イメージを構成して、記憶の負担を増やさないように加工を行っている。

【0065】図9は、ICカード12の通常利用を開始する前の設定に関する手順を示したものである。まず、利用者認証手続きを「海外利用モード」で使用するかを選択する(ステップ91)。次に、利用者固有の日本語グループを選択する(ステップ92)。ステップ92では、グループを複数選択しても良いし、選択しなくても良い。例えば、「草冠の付く漢字と半濁点の付くカタカナ」等のように選択する。一つ以上選択した場合、利用者はそのグループを暗証情報としてICカード12に記憶しておき(ステップ93)、そのICカード12を小売店での支払いに使う際、利用者認証手続きにおける判断の基準とする。すなわち、表示された文字がそのグループに属している場合、それを選択する。

【0066】図10は、ターミナル装置13にICカード12を挿入してから、電子マネーを扱う取引までの手順の概要を示したフローチャートである。電子マネーを支払う側のICカード12は、まずターミナル装置13が正しい規格にあったものかどうかを判定し(ステップ101)、次にICカード12の利用者が正当な利用者であるかを判定する(ステップ102)。これらのチェックに合格した後、ICカード12は電子マネーをターミナル装置13へ提供して取引処理(ステップ103)が実現する。ステップ101、102のチェックに合格しなかった場合は、ICカード12側が判断して、電子マネーを使った商取引は許可しない。

【0067】図11は、ICカード利用者の認証の手順を、「日本語情報加工プログラム」のICカード12上およびターミナル装置13上での動作から詳細に示したものである。

【0068】まず、「日本語情報加工プログラム」がICカード上12で起動され、ICカード12内に配布されている「日本語情報」参照し、利用者認証に使う幾つ

かの文字を選択する(ステップ111)。例えば、10個の文字が選択されたとなると、「日本語情報加工プログラム」は、さらにそのうち幾つかの文字(10個以下の任意数個)を選んで、正しくない文字のイメージを生成する。これは利用者認証処理の際に、利用者に指定してもらったための文字であり、「日本語情報加工プログラム」の側では、文字イメージ生成と同時に、その正誤テーブルも作成して保持しておく(ステップ112)。この正誤テーブル作成時には、利用者固有の情報として登録されている日本語グループに属している文字があれば、これも正しくない文字として正誤テーブルに設定しておく。例えば、「にんべんの付く漢字」が登録されていれば、「信」の文字はイメージとして加工されていなくても、正しくない文字として設定しておく。生成した利用者認証情報は、文字イメージ情報のみを順番に、ICカード12からターミナル装置13へと送信する(ステップ113)。

【0069】ターミナル装置13では、これらを受信した後(ステップ114)、その複数の文字イメージを順番に画面表示装置23上に表示し(ステップ115)、利用者からの認証情報を受け付ける(ステップ116)。利用者は、表示された文字イメージを見て、その中で誤っている文字をターミナル装置13上で指定する。指定には、テンキーなどを利用する。また、画面表示装置23がタッチパネルになっている場合は、直接文字イメージに触れることで、指定できる。その他、各種ポインティングデバイスを使ってもよい。正当な利用者が指定すべき文字は、誤っているものだけでなく、以前に利用者固有の日本語グループとして予め登録しておいたものに属する文字も、指定する。利用者から指定された文字は、その番号情報がターミナル装置13からICカード12へと送信される(ステップ117)。

【0070】ICカード12では、「日本語情報加工プログラム」がターミナル装置13から送られた文字番号情報を受信し(ステップ118)、予めステップ112で作成しておいた正誤テーブルを使って認証を行い(ステップ119)、その判定結果をターミナル装置13へと送信する(ステップ710)。

【0071】ターミナル装置13は、ICカード12から認証判定結果を受信し(ステップ711)、そのメッセージ内容を、画面表示装置23内に用意しておいたメッセージ用のエリア55に表示する(ステップ712)。

【0072】この後、ターミナル装置13では認証結果が成功か否かを判定し(ステップ713)、認証が成功した場合は、ICカード12へ利用者認証手続きの終了要求を送信する(ステップ717)。一方、認証が失敗した場合は、さらに「ある決まった回数まで」などの条件付きで再試行要求を利用者から受け付け(ステップ714)、再度、利用者認証を試みる場合は、ICカード

12へとそのメッセージを送信する(ステップ715)。再試行しない場合は、認証が成功した場合と同様、終了要求を送信する(ステップ717)。

【0073】「日本語情報加工プログラム」は、ターミナル装置13からメッセージを受信し(ステップ716)、再試行要求か、終了要求かを判断し(ステップ718)、前者の場合はもう一度ステップ111に戻り、後者の場合は利用者認証手続きを終了する。

【0074】図12は、ターミナル装置13内の画面表示装置23に表示された認証情報入力用の画面の例である。この画面は、図11のステップ115で表示され、テンキーなどを用いてステップ116で利用者から文字番号を受け付ける。この例では、8個の文字が表示エリア121に表示されており、そのうち1番、3番、4番の文字が、明らかに誤りとなっている。また、利用者固有の情報として、例えば「にんべんの付いた文字」のグループを登録してある場合は、7番が該当する。従って、利用者は1番、3番、4番、7番の4個の文字をここで指定することが要求される。

【0075】この他に画面内には、これまでどの文字を指定したかを確認するため、その番号をエコー表示するためのエリア122、文字を指定し終ったことを確定する時、これまでの指定をキャンセルする時、利用者認証の手続きを再試行する時などの操作を説明するガイド表示123、認証判定結果などを表示するためのメッセージ表示エリア124などが用意されている。

【0076】図13は、ターミナル装置13内の画面表示装置23に表示された認証情報入力用画面の2番目の例である。この画面も図12と同様、図11のステップ115で表示され、テンキーなどを用いてステップ116で利用者から文字番号を受け付ける。この例では、ヨーロッパ系言語のアルファベット中に含まれる8個の文字が表示エリア131に表示されており、カード利用者をドイツ語圏の人と想定して、母国語に含まれている文字を選択する状況を想定している。ドイツ語のアルファベットに含まれている文字は、表示されている8個の文字のうち、3番と7番だけであるから、正しいカード利用者はこれらを選択することを要求される。ここで、カード利用者がドイツ語圏の人であれば、日常的に用いている母国語の文字であるか否かは即座に判断できる。ここに例として選んだ文字は、いずれも他の言語のアルファベットに含まれる正しい文字であるが、図12の例のように既存の文字を加工して、どの言語にも含まれていない文字イメージをICカード12内で作り、ターミナル装置13上で表示することも可能である。

【0077】これら特定の母国語の文字セットをもとにした方法は、ヨーロッパ系言語に限らず、中国語、韓国語、東南アジア系言語、アラビア語など、様々な応用が可能である。

【0078】図14は、ターミナル装置13内の画面表

示装置23に表示された認証情報入力用画面の3番目の例である。この画面も図12と同様、図11のステップ115で表示され、テンキーなどを用いてステップ116で利用者から単語番号を受け付ける。この例では、北欧系のメーカー名や製品名などの9個の単語が、表示エリア141に表示されており、カード利用者をデンマーク人と想定して、母国のメーカー名や製品名ではないものを選択する状況を想定している。表示されている9個の単語のうち、2番、7番、9番はスウェーデンのメーカー名であるので、正しいカード利用者はこれらを選択することを要求される。ここで、カード利用者がデンマーク人であれば、日常的に広告媒体などで母国のメーカー名や製品名などには慣れ親しんでいるので、母国のものであるか否かは即座に判断できる。また逆に、母国のものだけを選ぶという設定にすることも可能である。さらに、他国に関連する単語だけでなく、母国に関連する単語についても、綴りや表記を図12の例のようにICカード内で加工して誤ったものを作り、ターミナル装置13上で表示することも可能である。

【0079】ここに例として選んだ単語は、酒類、通信、新聞、製菓、たばこ、家具、玩具、食器など身の回りに関係するものであるが、本発明はそれらの分野に限定されるものではない。

【0080】図15は、ターミナル装置13内の画面表示装置23に表示された認証情報入力用画面の4番目の例である。この画面も図12と同様、図11のステップ115で表示され、テンキーなどを用いてステップ116で利用者から単語番号を受け付ける。この例では、利用者のよく知っている勤務地付近の地域情報に基づく9個の単語が、表示エリア151に表示されており、カード利用者は、自分の勤務地付近にないものを選択する状況を想定している。表示されている9個の単語のうち、2番と6番は他と比べて離れているので、正しいカード利用者はこれらを選択することを要求される。ここで、カード利用者は勤務地付近の地域情報には日常的に慣れ親しんでいるので、勤務地付近にあるものか否かは即座に判断できる。また逆に、自分の勤務地付近のものだけを選ぶという設定にすることも可能である。さらに、付近以外の単語を混ぜて利用するだけでなく、勤務地付近の地域情報に関連する単語についても、一部の文字を取り替えるなどして図12の例のようにICカード内で加工して誤ったものを作り、ターミナル装置13上で表示することも可能である。

【0081】選択する地域としては、勤務地以外にも、出身地、親戚のいる地域、出身学校周辺など、ICカード利用者が既にその地域に詳しいようなものを選ぶ。

【0082】ここに例として選んだ地域情報としては、公共施設、小売店、交通関係、宿泊施設、観光スポットなどであるが、本発明はそれらの分野に限定されるものではない。

【0083】認証情報として利用する地域情報は、1つの地域だけであると、通常その地域情報に詳しい者がたくさんいるので、予め複数の地域を選んでおき、図15と同様の認証情報入力用画面をそれぞれ使って、複数地域に関する認証情報の入力を行い、選択したすべての地域に詳しい者がICカード利用者にほとんど限定できるようにしておく。

【0084】認証用の地域情報をICカード利用者に特化するには、対象とする地域を狭めて、細かいレベルの情報に限定したり、ICカード利用者のみが知っている情報を混せてICカードへ貯えておく。

【0085】ICカードに貯えておくべきICカード利用者固有のデジタル化された地域情報は、例えばカーナビゲーションシステム、地図情報システムなどから、その一部を認証用の情報として利用できるが、本発明はその情報の取得方法を限定するものではない。

【0086】図15の方法によれば、海外利用に限らず、国内利用においてもICカード利用者認証に充分効果がある。

【0087】以上のように、ICカード利用者は銀行のキャッシュカードの暗証番号を覚えるのと同程度の負担で、複雑な暗証情報を利用できる。

【0088】また、このような母国語情報に基づいたバリエーションの豊かな認証情報入力用の画面を利用することにより、海外で暗証情報を入力する際に、まわりにいる人間に情報を盗まれる可能性や、ターミナル装置13に隠された装置で盗聴される可能性を非常に少なくできる。また、利用者にとって固有の情報も、暗証番号の増加に比較して少ない記憶量の負担で、セキュリティ面での大きな効果が期待できる。

【0089】以上の説明から明らかなように、本実施形態によれば、ICカードを利用した商取引サービスにおいて、海外利用と国内利用のリスクの差を埋めるために、以下の特徴を持つ、ICカードの利用者認証を補助する方式を実現できる。

(1) ICカードの国内利用または国際的な商取引の様々な状況において暗証情報を盗むことを困難にすることができる。

(2) ターミナル装置に付加すべき暗証情報読み取り用として、特定の暗証情報の種類に特化した特殊装置を必要としない。

(3) 暗証情報の増加や複雑化に伴う利用者への負担を増やさない。

【0090】これらの特徴は、ICカードを利用する状況が、国内外を問わずレストラン、スーパーマーケット、駅の売店、タクシー、アミューズメントセンターなど、一律にセキュリティの水準を確保することが困難な、様々なものへと広まった際に、特に有効なものとなる。

【0091】

【発明の効果】以上のように本発明によれば、ICカードを利用した商取引サービスにおいて、海外利用と国内利用のリスクの差を埋めるために、以下の特徴を持つ、ICカードの利用者認証を補助する方式を実現できる。

(1) ICカードの国内利用または国際的な商取引の様々な状況において暗証情報を盗むことを困難にすることができる。

(2) ターミナル装置に付加すべき暗証情報読み取り用として、特定の暗証情報の種類に特化した特殊装置を必要としない。

(3) 暗証情報の増加や複雑化に伴う利用者への負担を増やさないなど、ICカード利用者のみが持つ暗証情報を、利用者の記憶等の負担を増やすことなく、しかも盗聴行為に対して安全にICカード側で受け取り、認証することができる。

【図面の簡単な説明】

【図1】本発明のICカード向け利用者認証方式を実現する基盤となる、サービス提供者、ICカード、ターミナル装置の3者の関係を示した図である。

【図2】ICカード向けターミナル装置の一実施形態を示す外観構成図である。

【図3】ターミナル装置にICカードを挿入してから、電子マネーを扱う取引までの手順の概要を示したフローチャートである。

【図4】ICカード利用者の認証の手順を詳細に示したフローチャートである。

【図5】暗証情報受付プログラムによって表示された認証情報入力用の画面の例を示した図である。

【図6】2つのプログラムの間で受け渡される暗証情報のデータフォーマットの例を示した図である。

【図7】ICカード内に保存しておく「日本語情報」の例である。

【図8】日本語情報加工プログラムにより、容易に誤りと判定できる文字イメージの生成例を示す図である。

【図9】ICカードの通常利用を開始する前の設定に関する手順の概要を示したフローチャートである。

【図10】ターミナル装置にICカードを挿入してから、電子マネーを扱う取引までの手順の概要を示したフローチャートである。

【図11】ICカード利用者の認証の手順を詳細に示したフローチャートである。

【図12】ターミナル装置上に表示された認証情報入力用の画面の例を示した図である。

【図13】ターミナル装置上に表示された認証情報入力用の画面の例を示した図(その2)である。

【図14】ターミナル装置上に表示された認証情報入力用の画面の例を示した図(その3)である。

【図15】ターミナル装置上に表示された認証情報入力用の画面の例を示した図(その4)である。

【符号の説明】

17

18

12...ICカード、13...ターミナル装置、23...画面表示装置、71...日本語情報、121...暗証情報受付プログラム、

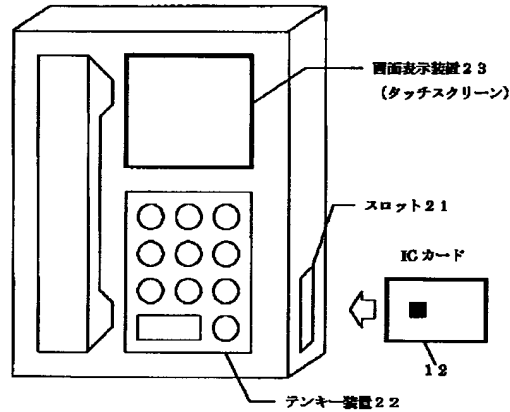
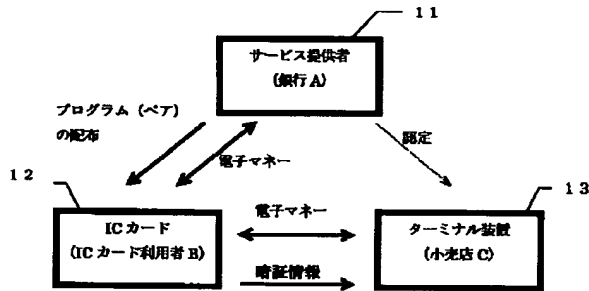
ログラム、122...暗証情報認証プログラム。

【図1】

【図2】

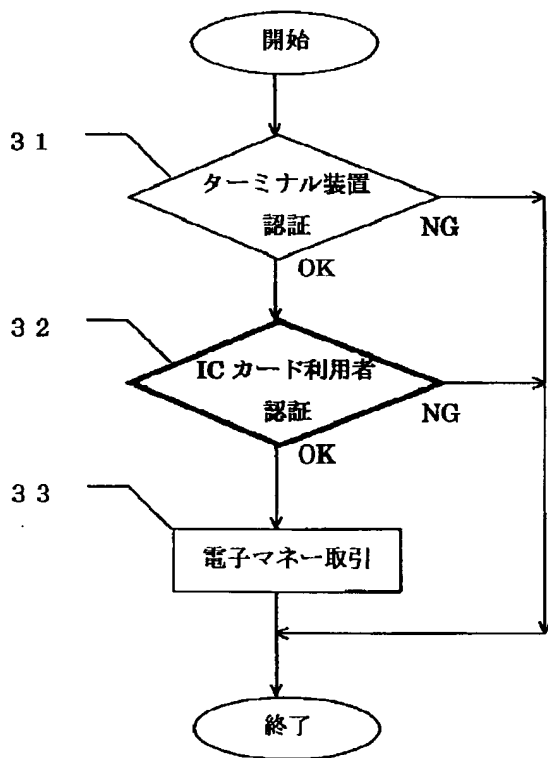
図 1

図 2



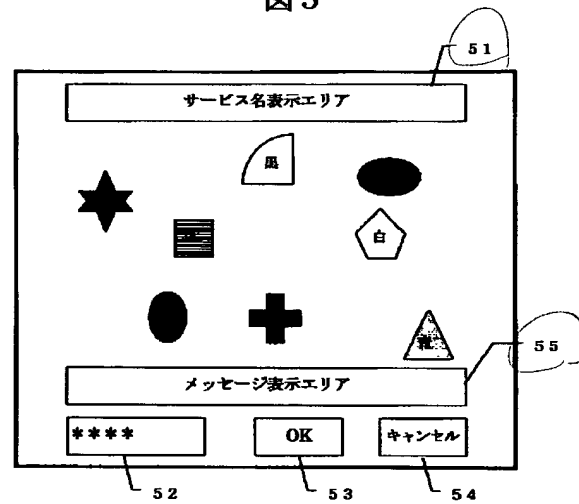
【図3】

図 3



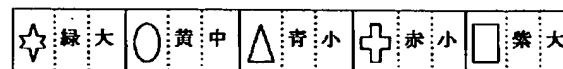
【図5】

図 5



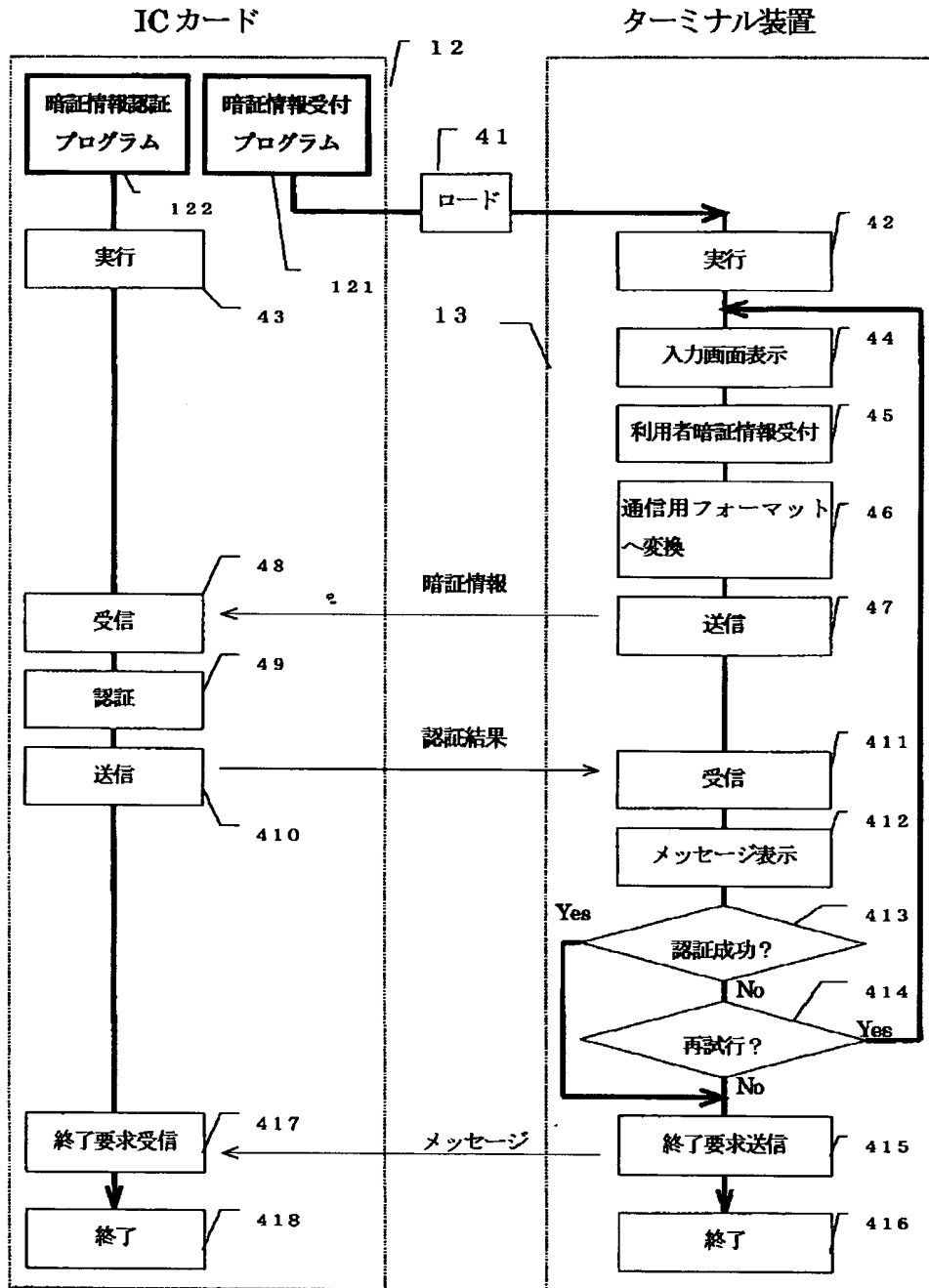
【図6】

図 6



【図4】

図 4



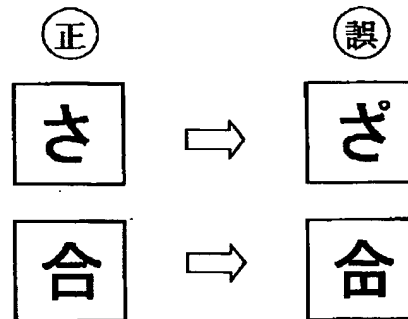
【図7】

図 7

番号	イメージ	部首	画数	種類	漢字
1	佐	にんべん	7	漢字	—
2	ジ	—	5	カタカナ	有
3	あ	—	3	ひらがな	無
...

【図8】

図 8

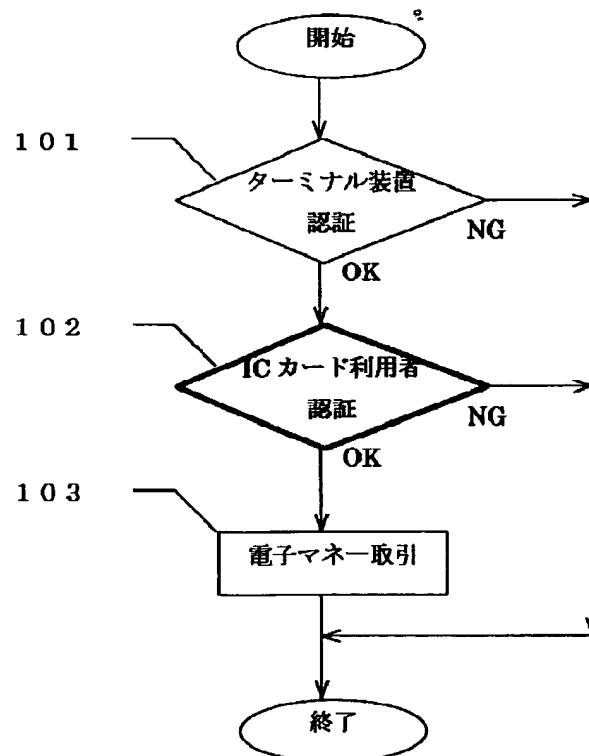
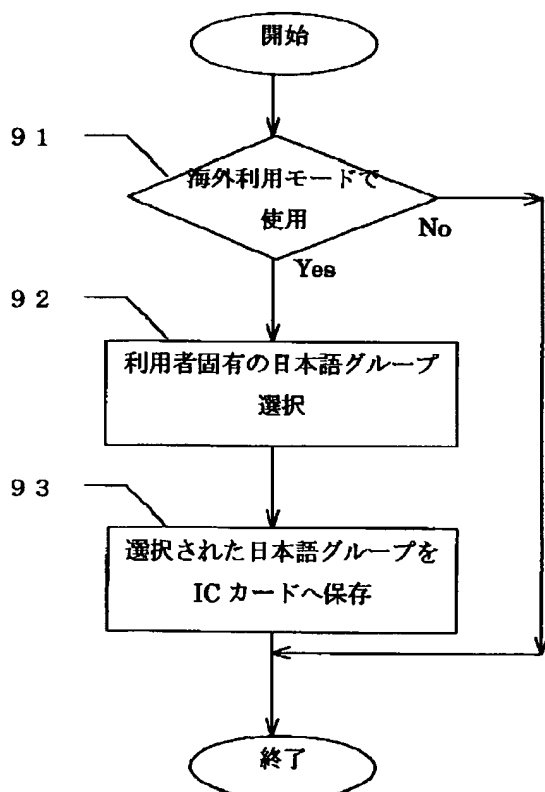


【図10】

図 10

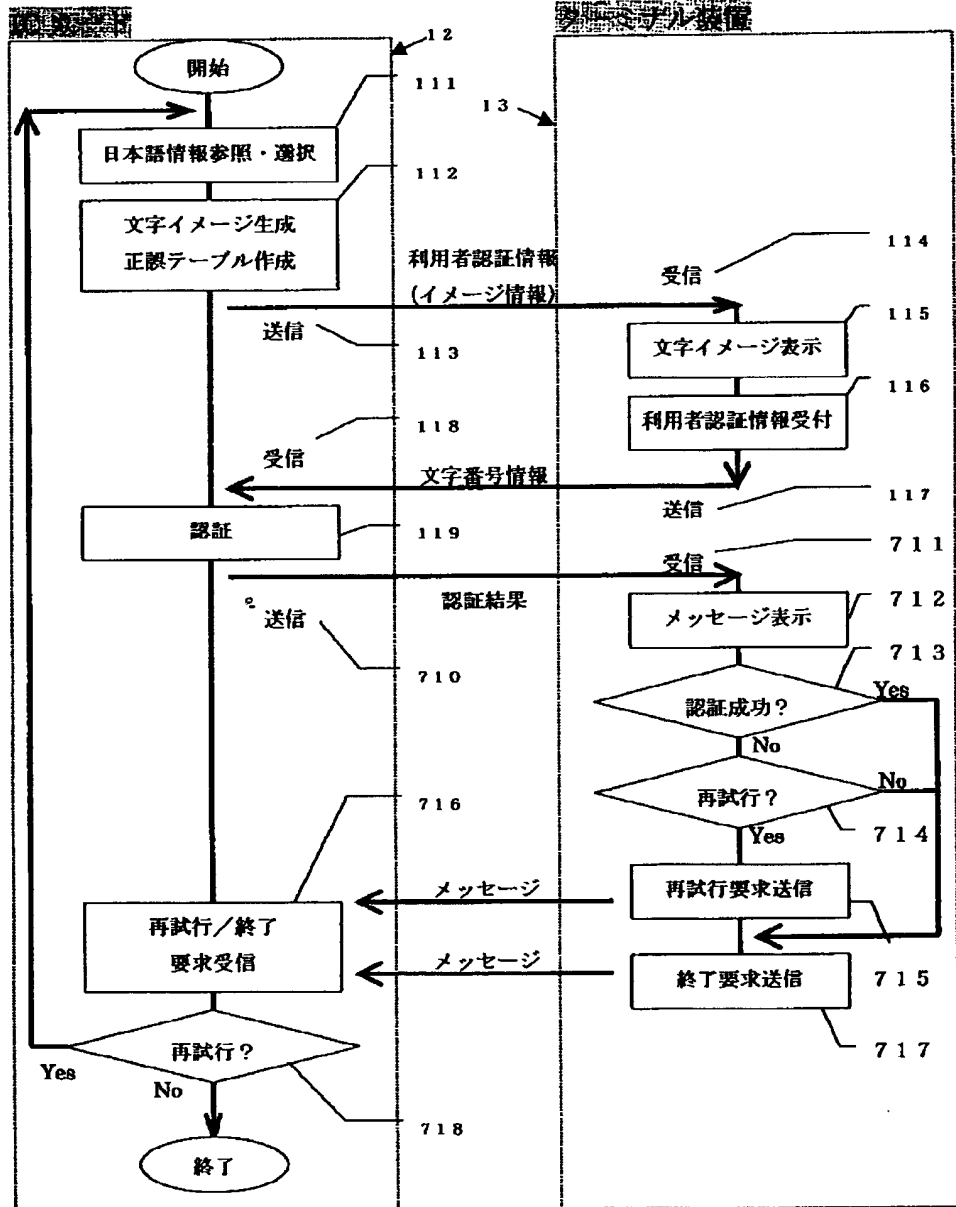
【図9】

図 9



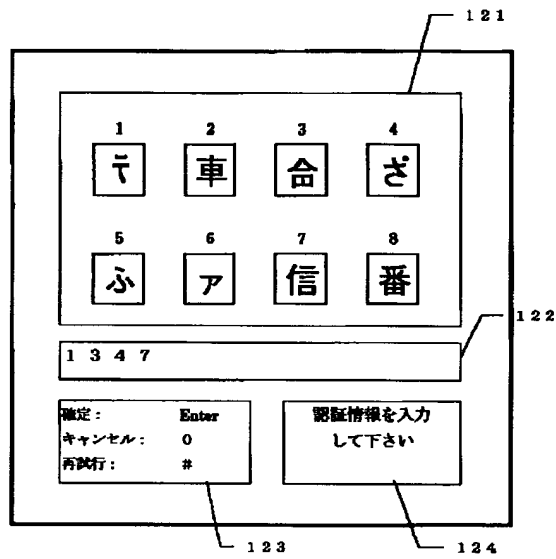
【図11】

図 1 1



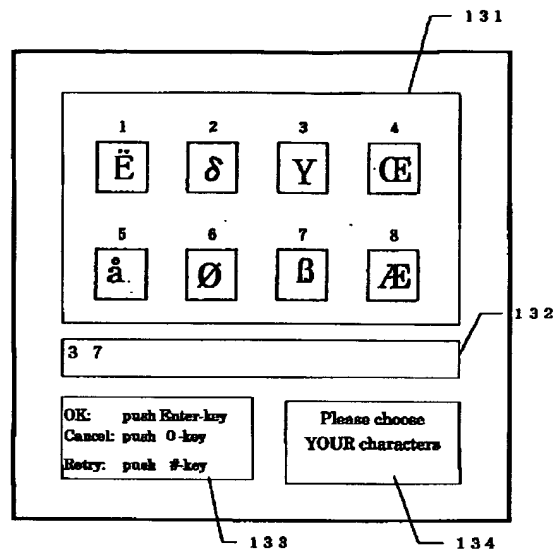
【図12】

図12



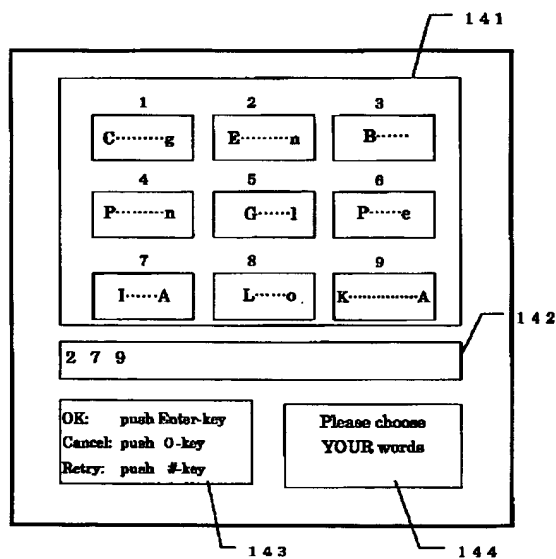
【図13】

図13



【図14】

図14



【図15】

図15

